IN THE SPECIFICATION

Please amend the specification as follows:

On Page 4 Of The Specification

Prior to the first full paragraph on page 4 of the Specification, please insert the following:

--Advances in network technology and widespread availability of high speed access to the Internet have led to a rapid increase in the use of online services. Although a paperless society may never be fully realized, more and more records are being maintained and accessed electronically over the Internet. Financial and medical records are among the most sensitive of these records and require the most diligence for security, prevention of unauthorized access, and alternation or manipulation.

In many cases, the privacy of medical and financial online records is the subject of stringent government regulations. For example, the Health Insurance Portability and Accountability Act (HIPAA) regulates the use and disclosure of medical records held by health insurers, medical service providers and the like, and places serious civil and criminal sanctions on violations. The Right to Financial Privacy Act of 1978 places restrictions on a bank's disclosure of customer records to government agencies. Even the European Union has imposed a comprehensive privacy regime for personal electronic data with which U.S. and other non-EU commercial interests must comply.

Custodians and users of online records subject to disclosure regulations are under a heavy burden to observe privacy requirements while simultaneously being responsive to legitimate inquires for uses of such records. For example Congress enacted the Health Information Technology for Economic and Clinical Health (HITECH) Act as part of the American Recovery and Reinvestment Act on February 17, 2009. The HITECH Act requires health care providers and other HIPAA-covered entities promptly to notify affected individuals of a breach, as well as the HHS Secretary and the media in cases where a breach affects more than 500 individuals.

Within an ever complex and changing privacy regulatory environment it is not often clear to average users, unfamiliar with the legal nuances of regulatory environments, the scope of information that is covered by the regulations and thus they may inadvertently breach covered information without the means to determine that the information breached was covered and now has a reporting requirement attached.

A number of approaches are known in the prior art for managing disclosure of health care information among interest parties, such as health care providers, patients and insurance companies. One such approach is described in Patent Application disclosure No. 2004/0220829 in the name of Baharav et al. and is entitled “Distributed System and Method For Managing Communication Among Healthcare Providers, Patients and Third Parties.” However, the Baharav et al system does not provide any way to encrypt medical records to ensure their privacy or provide an effectively way to prevent their access by unauthorized parties. Moreover, the Baharav et al system provides no method of non-repudiation where the sender of a message can not later deny having sent the message and the recipient can not later deny having received the message.

U.S. Patent No. 6,480,850 issued in the name of Veldhuisen and is entitled “System And Method For Managing Data Privacy In A Database Management System Including A Dependently Connected Privacy Data Mart.” This patent is directed to a data warehouse and in particular, to a method and apparatus for collecting and analyzing data and providing such analyzed data to data consumers. The information stored in the warehouse is collected from commercial transactions between retail outlets and retail consumers. Analyzing vast amounts of such information can be used to determine purchasing trends, consumer taste and the like. The information may also be correlated to personal information about a consumer such as age, occupation, income, etc.

The Veldhuisen system proves some degree of privacy for personal information and the ability of the owner of the information to establish privacy preferences and to correct erroneous information. The system, however, does not take into account, and can not easily implement, privacy protocols and rules that are mandated by government regulations. Veldhuisen, like the Baharav et al system described above, also provides no method of non-repudiation of send and received messages.

Further, since such systems using prior art involve the replication of databases and the creation of additional metadata connected to the original database; accessible remotely by any consumer, such replication and creation enhances risks of data breaches and database corruption. HIPAA and other privacy rules and regulations require prompt notification of breaches, and statutes enacted in some States, such as California, prescribe serious penalties for failing to report such breaches and existing common law duties of care may support individual and civil class action liability for data losses or breaches.

Thus, prior art approaches to computer and network security that may have been sufficient in the past are not adequate for today's need to store and access vast amounts of sensitive financial, personal, and medical records that are stored electronically including remotely, on a variety of non interoperable systems subject to complex statutory schemes and regulatory requirements that often require legal interpretation prior to electronic implementation. --

On Page 7 Of The Specification

Prior to the last full paragraph on page 7 of the Specification, please insert the following:

--The method and apparatus for securing the privacy of a computer network in accordance with the present invention includes a number of key features, including a programmable, secure hardware key that embodies a data encryptor and a device identity (via a static IP address or similar means) for each assigned user, with embedded unique identity roles and permissions reflective of the assigned user's role and responsibility, respectively.

The hardware key assigned to each user, in turn, is embedded with algorithms, that imprint indelible electronic tags that comport with privacy rules and regulations and provide recognition events that appear on a user's screen as a notification or alert, reflecting current, applicable legal and regulatory requirements, all of which can be updated, as necessary when new statutes are passed and new regulations promulgated, through a central secure server operated by BPN or other central administration authority.

The hardware key is agnostic and adaptable. It thus works with and is adaptive to any installed system, regardless of relational or non-relational database structure, and does not alter or affect data stored in any way, thus eliminating any liability for data loss or elimination, and thus creating a new potential standard of care in data integrity.

The ability of the invention to link securely previously non-interoperable databases facilitates the coordination of health information and personal health records, which in turn, enables new coordinated care delivery paradigms; such as Medical Homes; to be implemented more readily and at lower costs.

The hardware key includes a nonrepudiation identity feature which, in turn, allows an audit trail of each user's individual key activities, thus complying with U.S. and E.U. privacy legislation requirements.

The ability of the keys to securely link previously non interoperable data bases inventively facilitates the coordination of health information and personal health records which in turn enables new care delivery paradigms; such as Medical Homes; to be implemented more readily and at lower costs.--

IN THE CLAIMS

This listing of the claim will replace all prior versions and listings of claim in the present application.

Listing of Claims

1. (Originally Presented) A method of secure privacy notification, said method comprising the steps:

determining the regulatory compliance requirements for privacy notification of data subjects;

transforming said requirements into electronic and non-electronic database query screens and forms;

querying a remote and/or resident database for information fields contained within said query screens and forms;

human or automated completion of said data screens;

encryption/decryption of said data screens;

human and/or automated conversion of data screens into privacy notification human readable formats;

electronic and/or non-electronic data subject feedback response methods and means; and

conversion of said data subjects feedback responses into database deletion, modification or correction of the data subject's information in accordance with said regulatory requirements.

2. (Originally Presented) The method of claim 1 wherein said electronic privacy notification and feedback response is accomplished via a secure web portal.

3. (Originally Presented) The method of claim 1 wherein said electronic privacy notification and feedback response is accomplished via a secure e-mail system.

4. (Originally Presented) The method of claim 1 wherein said electronic privacy notification and feedback response is accomplished using digital certificates comprising:

a public or private, commercial or government registration authority;

a public or private, commercial or government certificate authority;

a digital signature encryption algorithm'

a unique non-reputable user electronic identity;

issuance of x.509 compliant certificates specifically encoded via extension to alert data processor of the data subjects privacy preferences; and

issuance of x.509 standard certificates specifically encoded via extension to alert data processors of legal and regulatory compliance requirements relevant to the data subjects privacy preferences.

5. (Originally Presented) The method of claim 4 wherein said digital signature algorithm is SHA-1 with DSA.

6. (Originally Presented) The method of claim 4 wherein said digital signature algorithm is an elliptic curve.

7. (Originally Presented) The method of claim 6 wherein said elliptic curve is a Koblitz binary curve.

8. (Originally Presented) The method of claim 4 wherein said digital signature algorithm is a block cipher such as Rijndael.

9. (Originally Presented) The method of claim 4 wherein the data subjects privacy preference is to “opt out” and where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

10. (Originally Presented) The method of claim 4 wherein the data subjects privacy preference is to “opt in” and where encoding the digital certificate to be easily read by visual inspection by distinct color coding.

11. (Originally Presented) The method of claim 4 including third party archiving of certificate for non-repudiation, compliance audit and send and receive functions.

12. (Originally Presented) The method in claim 4 including the binding of a users identity and access authorizations to a physical device, such as a USB key, and challenging the key at a remote email server in order to gain access to the users authorized email box and messages.